MEDICAL DEVICE SECURITY ASSESSMENT THROUGH COMPUTATIONAL TECHNIQUE

Abstract Submitted to the
Babasaheb Bhimrao Ambedkar University, Lucknow
in Fulfillment of Requirement for the Award of Degree of

Doctor of Philosophy
in Information Technology

Submitted By
Masood Ahmad
Enrollment No. 675/18

Co-Supervisor
Dr. Rajeev Kumar
Assistant Professor at Centre for Innovation and Technology Administrative Staff College of India, Telangana

Supervisor
Prof. Raees Ahmad Khan

Department of Information Technology
School of Information Science & Technology,
Babasaheb Bhimrao Ambedkar University, (A Central University)
Lucknow, Uttar Pradesh-226025

2022

ABSTRACT

E-health is a developing field that uses wireless sensor networks to provide access to effective and efficient healthcare services as well as patient monitoring to aid in the early detection and treatment of health conditions. This allows for remote monitoring and reprogramming of the patient's devices. Because of the proliferation of e-health systems, data falsification, unauthorised system access, and eavesdropping on sensitive health data have become critical issues. Furthermore, security and device performance can be difficult to balance due to the inherent limitations of many wireless medical devices, such as low power and limited computational resources. As a result, many current networked medical devices lack basic security services like authentication, authorization, and encryption.

Healthcare devices are critical in tracking and managing patient safety. However, due to network, hardware, and software, healthcare system issues, the complexities of healthcare devices frequently remain ambiguous. Targeting healthcare is primarily motivated by two factors: first, healthcare data contains all the transactions and patient’s history, which is the most valuable entity on the dark web, and second, it is the soft target. Healthcare data breach has become a major risk for healthcare organizations because they break the confidentiality of the organization, with hackers demanding ransom and threatening to reveal healthcare information if not paid within the specified time frame.

The vast majority of the medical device in use today lacks built-in security features. As a result, whether connected to the network, these medical devices' inherent flaws make them vulnerable to a wide range of cyberattacks. Hackers can take a device under control and make the hotspot, manipulate data, and disrupt facilities in hospitals and clinics. A professional can manage cybersecurity threats by reducing the system's attack surface. Security analysis is critical in risk mitigation, whether it is used to detect potential vulnerabilities that attackers can exploit or prevent cyberattacks. Furthermore, security checks are required during the pre-market and post-market phases.

Medical device security is critical in e-healthcare today, and there has been a rapid increase in the use of networked devices in current healthcare services. However, these implantable devices are extremely vulnerable to attackers who are constantly targeting the security of devices in order to gain access to the patient's data. Infringement of patients' data is not only a violation of their confidentiality and integrity, but it can also endanger their lives if any little bit changes in their diagnosis report. Once the device has been gain accessed, attackers can switch off all network-connected medical devices. Vendors are not focusing on the security of the medical device, because organizations want the cheap product. But medical device security is a very serious topic because these are not only data breaches but are also connected with the life of patients. In this category, this thesis employs an integrated methodology to assess the security of medical devices at the pre and post-market phases. The study uses expert opinions to examine the security flaws in medical devices. Authors set criteria, sub-criteria and goals in a hierarchical format for assessing the security flaws in the devices by deep studying of the literature.

The current study discusses the various methods used to secure healthcare devices and proposes a quantitative framework for ranking their importance. To classify the best alternatives to security techniques for healthcare devices, the study employs the Hesitant Fuzzy (HF), Analytic Hierarchy Process (AHP), and Fuzzy Technical for Order Preference by Similarities to Ideal Solution (TOPSIS). According to the ranks of the alternatives acquired, A1 was the most likely of all the alternatives. This means that the security of A2 healthcare devices is the best of all options considered. The findings generated with the help of the proposed framework will serve as a corroborative guide for developers and manufacturers in quantitatively determining the security of healthcare devices in order to engineer effective devices. The assessments carried out with the proposed framework are systematic, precise, and conclusive. As a result, the current empirical analysis provides a more reliable and accurate choice than the manual assessment of the device's security.

Following that, we propose a framework for evaluating medical device security. In this regard, we present a. For selecting or ranking the MD, we propose a Hesitant

Fuzzy AHP-TOPSIS-based methodology. We chose attributes, security measures, and alternatives to assess the security of medical devices. Where HF AHP is used to prioritise security attributes and TOPSIS is used to calculate the impact of security factors on various alternatives. The technique is used to rate the alternatives based on how satisfied they are with their weights. As a result, the order of priority for the techniques is determined by the ranks of the alternatives. In addition, sensitivity analysis and validation are performed in the final phase.